IN THE CLAIMS

1-25. (Cancelled)

26. (Previously Presented) A method for processing frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

receiving a first frame at the first network entity from the second network entity in the fibre channel network, wherein the first frame is associated with a fabric login (FLOGI) or port login (PLOGI) message;

identifying a security enable parameter in the first frame, wherein the security enable parameter is used by the second network entity, when the second network entity is added to the fibre channel network, to determine if the first network entity has authentication capability or supports other security functions;

transmitting an acknowledgment to the second network entity that the first network entity has authentication capability or supports other security functions, the acknowledgment including algorithm information and a salt parameter;

receiving a second frame at the first network entity from the second network entity;

identifying a security control indicator in the second frame from the second network entity, wherein the security control indicator is used to determine if the second frame is encrypted or authenticated;

determining at the first network entity that a security association identifier associated with the second frame corresponds to an entry in a security database;

decrypting a first portion of the second frame by using algorithm information contained in the entry in the security database.

27. (Original) The method of claim 26, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

28. (Original) The method of claim 27, wherein the first portion is decrypted using a key contained in the entry in the security database.

29. (Original) The method of claim 27, wherein the first portion is encrypted using DES, 3DES or AES.

30. (Previously Presented) The method of claim 27, further comprising:

recognizing that a second portion of the second frame supports authentication;

using algorithm information contained in the entry in the security database to authenticate the second portion of the second frame.

31. (Original) The method of claim 30, wherein the second portion is authenticated using MD5 or SHA1.

32. (Original) The method of claim 30, wherein the authentication sequence is a fibre channel login sequence between the first and second network entities.

33. (Original) The method of claim 32, wherein the login sequence is a PLOGI or FLOGI sequence.

34. (Original) The method of claim 32, wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence.

35. (Original) The method of claim 32, wherein the first and second network entities are domain controllers and the authentication sequence is a SW_ILS sequence.

36. (Currently Amended) A method for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

transmitting a first fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity, the first fibre channel frame including a security enable parameter~~indicator~~, wherein the first fibre channel frame is associated with a fabric login (FLOGI) or a port login (PLOGI) message, wherein the security enable parameter is used by the first network entity, when the first network entity is added to the fibre channel network, to determine if the second network entity has authentication capability or supports other security functions;

receiving an acknowledgment from the second network entity indicating that the second network entity has authentication capability or supports other security functions, the acknowledgement including key and algorithm information and a salt parameter;

inserting key and algorithm information from the second network entity into a security database;

identifying a second fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

determining if the second fibre channel frame corresponds to the selectors of an entry in a security database;

encrypting a first portion of the second fibre channel frame using key and algorithm information associated with the entry in the security database;

providing a security control indicator in the second fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted or [[and]] authenticated;

transmitting the second fibre channel frame to the second network entity.

37. (Original) The method of claim 36, wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities.

38. (Original) The method of claim 36, wherein the payload is encapsulated using the Authentication Header protocol or the Encapsulating Security Payload protocol.

39. (Previously Presented) The method of claim 38, further comprising adding security information to the header of the second fibre channel frame.

40. (Previously Presented) The method of claim 37, wherein a first portion of the second fibre channel frame is encrypted using DES, 3DES, or AES.

41. (Previously Presented) The method of claim 37, wherein parameters in the header are normalized prior to encrypting the first portion of the second fibre channel frame.

42. (Previously Presented) The method of claim 41, wherein the payload is padded prior to encrypting the first portion of the second fibre channel frame.

43. (Previously Presented) The method of claim 37, further comprising:

computing authentication data using key and algorithm information as well as a second portion of the second fibre channel frame.

44. (Original) The method of claim 43, wherein authentication data is computed using MD5 or SHA1.

45. (Original) The method of claim 43, wherein the authentication sequence is a fibre channel login sequence between the first and second network entities.

46. (Original) The method of claim 45, wherein the login sequence is a PLOGI or FLOGI sequence.

47. (Original) The method of claim 45, wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence or an SW_ILS message.

48. (Currently Amended) An apparatus for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the apparatus comprising:

means for transmitting a first fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity, the first fibre channel frame including a security enable parameter~~indicator~~, wherein the first fibre channel frame is associated with a fabric login (FLOGI) or a port login (PLOGI) message, wherein the security enable parameter is used by the first network entity, when the first ~~second~~ network

entity is added to the fibre channel network, to determine if the second ~~first~~ network entity has authentication capability or supports other security functions;

means for receiving an acknowledgment from the second network entity indicating that the second network entity has authentication capability or supports other security functions, the acknowledgement including key and algorithm information and a salt parameter;

means for inserting key and algorithm information from the second network entity into a security database;

means for identifying a second fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity;

means for determining if the second fibre channel frame corresponds to the selectors of an entry in a security database;

means for encrypting a first portion of the second fibre channel frame using key and algorithm information associated with the entry in the security database;

means for providing a security control indicator in the second fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted or authenticated;

means for transmitting the second fibre channel frame to the second network entity.

49-50. (Cancelled)